Section IV: **Network Security**
Title: **Wireless Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **May 7, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To prevent unauthorized access to the North Carolina (NC) Department of Health and Human Services (DHHS) technology systems, specifically through the Institute of Electrical and Electronic Engineers (IEEE) 802.11 wireless communications, from eavesdropping on electronic signals.

STANDARD

1.0 Background

Wireless networks enable computers to be inter-connected using standard network protocols such as Internet Protocol (IP). Wireless networking technology relies on radio frequencies and data transmissions. The most widely used wireless standard is the IEEE 802.11, which has been adopted by the NC State Office of Information Technology Services (ITS) to serve as the statewide wireless standard.

The wireless security standards are addressed in the NC Statewide Information Security Manual, Version No. 1 **–** Chapter 9 **–** Dealing with Premises Related Considerations, Section 03: Other Premises Issues **–** Standard 090301 – Electronic Eavesdropping. In addition, this standard will address ten (10) areas of wireless configurations. The following ten (10) areas are listed in the statewide approved Wireless Security Standard:

1. **Physical Access**

   - All network access points (APs) and related equipment, such as base stations and cabling, supporting wireless networks shall be secured with locking mechanisms or kept in a secured area where access is restricted to authorized personnel.
   - The reset function on APs shall only be used by and accessible to authorized personnel.

2. Network Access

- All APs shall be segmented from an internal wired local area network (LAN) using a gateway device or service.
- The service set identifier (SSID) must be changed from the default value.
- The SSID shall not contain characters that indicate the location of the wireless LAN (WLAN) AP (e.g., the name of the Division and Office and/or any other identifying name).
- The SSID broadcast function shall be disabled except where technology does not permit. In cases where the SSID broadcast function cannot be disabled the Network Administrator must notify the Division Information Security Official (ISO) in writing.
- A device shall not be connected to a wireless network unless it can provide the valid SSID.

3. System Access

- Every device used to access the state's network over an IEEE 802.11 wireless connection must utilize a personal firewall (software or hardware) and up-to-date anti-virus software (devices incapable of running anti-virus or personal firewall software such as radio frequency identification (RFID) tags, voice telephony systems, or personal digital assistants (PDAs) are exempt from this requirement).
- All access points shall require a password to access its administrative features. This password shall be stored and transmitted in an encrypted format only. Passwords shall be changed every thirty (30) days, as per the NC Statewide Information Security Manual, Statewide Information Technology Standard, Version No. 1 – August 2004, User Identification (ID) and Password Protection Standard.
- The ad-hoc mode for IEEE 802.11 referred to as peer-to-peer mode or independent basic service set (IBSS) must be disabled. The ad-hoc mode shall be allowed only in the narrow situation in which an emergency temporary network is required. Every device used to access the state's network, over an IEEE 802.11 wireless connection, when not in use for short periods of time, must be locked (via operating system safeguard features), and shall be turned off when not in use for extended periods of time, unless the device is designed to provide or utilize continuous network connectivity. Such items may include wireless cameras, RFID tag readers, and other portable wireless devices.
- If supported by the devices, auditing features on wireless devices shall be enabled and reviewed periodically by designated staff.

4. Authentication

- All wireless access to the state's network via an IEEE 802.11 wireless network shall be authenticated by requiring the user to supply the appropriate credentials. In addition, authentication shall be performed through such technologies as secure socket layer (SSL), secure shell (SSH), or virtual private network (VPN) when a LAN is extended or a wide-area network (WAN) is created using IEEE 802.11 wireless technologies.
- The IEEE 802.1x credentials for individual users shall be deactivated in accordance with an agency's User Management policy or within twenty-four (24) hours of notification of a status change (e.g., employee termination or change in job function).

5. Encryption

- Depending on the type of information traversing a WLAN, encryption is required at various levels, as noted in Section 9: Wireless LAN Defense-In-Depth Architecture, below. At a minimum, public information requires Wi-Fi Protected Access (WPA) encryption and protected data requires IEEE 802.11i (WPA2) compliant Advanced Encryption Standard (AES). End-to-end encryption is highly recommended for confidential data.
- Wired Equivalent Privacy (WEP) shall not be used for wireless security.
- When WPA is used, the highest level of encryption supported on the device must be enabled.
- WPA encryption must at least use Temporal Key Integrity Protocol (TKIP), other IEEE, or National Institute of Standards and Technology (NIST) approved key exchange mechanism. Advanced Encryption Standard (AES) is the preferred encryption standard to use.
- When WPA2 is used, AES encryption shall be enabled and must be no less than 128-bits.
- WPA2 encryption must use Cipher Block Chaining Message Authentication Code Protocol (CCMP), other IEEE, or NIST-approved key exchange mechanism.
- When end-to-end encryption is required across both an IEEE 802.11 wireless and a wired network, then, in addition to WPA2 (IEEE 802.11i), data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality per the NC Statewide Information Security Manual. Such protocols may include the following: SSL, SSH, IP Security (IPSec), VPN tunnel, etc.
- Pre-shared keys shall be strong in nature, randomly generated, and redistributed to users at least quarterly to protect against unauthorized shared-key distribution or other possible key exposure situations. These keys will be treated in the same manner as passwords and the keys must consist of a minimum of eight (8) characters. The keys must meet or exceed the state password standards in complexity when possible and must be changed every ninety (90) days to ensure confidentiality. Pre-shared keys sent by email must be encrypted.

6. Wireless System Management

- The Simple Network Management Protocol (SNMP) shall be disabled if not required for network management purposes.
- If required for network management purposes, SNMP shall be read-only with appropriate access controls that prohibit wireless devices from requesting and retrieving information.
- If SNMP is required for dynamic reconfiguration of access points to address AP failures and rogue APs, use the SNMP Version 3 (or higher) protocol and only on the wired side of the network. The latest version of SNMP Version 3 supported by both devices and management stations shall be implemented. Support for earlier versions of SNMP shall be disabled.
- Pre-defined community strings such as *public* and *private* keys shall be changed to a unique name.
- IEEE 802.11 wireless devices shall not be used to manage other systems on the network except in temporary, ad-hoc, and emergency situations or by the use of end-to-end encryption with authentication.

7. WAN Connections

Authentication shall be performed when point-to-point wireless access points are used between routers to replace traditional common carrier lines.

8. Audit

- The Divisions and Offices using IEEE 802.11 WLANs must enable rogue AP detection in the WLAN management software and search their sites using wireless sniffers at least monthly to ensure that only authorized wireless APs are in place. A current list should be maintained for all authorized APs.
- Similarly, these types of audits are recommended for sites not using wireless technologies to detect rogue APs and end-user installed free-agent APs.
- The management system shall monitor the airspace in and around Divisions and Offices for unauthorized APs and ad-hoc networks. If unauthorized devices are found, then the Division and Office ISO should take appropriate steps toward containment.

9. Wireless LAN Defense-In-Depth Architecture

Access	Isolated WLAN	Credential Management	Rotating SSID/PSK	WPA w/ Strong PSK	WPA2 w/ Strong PSK	802.11i w/ 802.1x*	Encryption	VPN	Personal Firewall + AV **
Open WLAN for On-Site Citizen Use	Firewall**	SSID	Required	-	-	-	-	-	-
Public Information	WLAN Gateway	PSK	Required	Required Minimum	Recommended	-	Required	-	Required
Confidential Information	WLAN Gateway	802.1x	-	-	Required	Minimum	Required	Recommended	Required
Access into Agency Network from Wi-Fi Hot Spot by State Employees/ Contractors	-	VPN	-	-	-	-	-	Required	Required

* Third-party or vendor-specific WLAN security solutions that provide equivalent levels of authentication and encryption are acceptable.
** PDAs and other devices incapable of running personal firewall and anti-virus software are exempt from this requirement.

10. Divisions and Offices Reporting Requirements

- In accordance with the NC Statewide Information Security Manual, agencies shall report all IEEE 802.11 WLANs to the State Chief Information Officer (State CIO).

- This reporting process will be sent to the DHHS Privacy and Security Office (PSO), which will then forward the wireless information to the State CIO.

2.0 Division and Office Management and Security

The Divisions and Offices shall ensure that:

- Only authorized users are allowed to utilize wireless communications
- Only authorized entities are allowed to install wireless communications
- The use of non-approved methods, devices, technologies, or means of communications shall be prohibited
- All authorized workforce members have signed the corresponding agreements and have completed training
- All workforce members are in compliance with statewide policies, procedures, standards, and guidelines, as well as other federal and state regulations

The Division ISO is responsible for managing and maintaining pre-shared keys for encryption. Logging of the assigned keys will be maintained by the Division ISO and will be subject to an audit.

The Division ISO is responsible for providing security oversight for compliance with this standard and reporting security-related incidents to DHHS PSO. The Division ISO is required to perform internal audits on a routine and periodic basis to ensure full compliance.

The Division ISO shall be responsible for approving wireless devices and/or projects. Once the devices and/or projects have been deployed, but prior to utilization, the PSO will be notified and will scan/review the installation for compliance with this standard.

Reference:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 2 – Controlling Access to Information and Systems, Section 01: Controlling Access to Information and Systems
    - Standard 020101 – Managing Access Control Standards
  - Chapter 9 – Dealing with Premises Related Considerations, Section 03: Other Premises Issues
    - Standard 090301 – Electronic Eavesdropping

- NC Statewide Information Security Manual, Statewide Information Technology Standard, Version No. 1 – August 2004
  - User Identification (ID) and Password Protection Standard

- NC DHHS Security Standards
  - Network Security Standards
    - Encryption Security Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - Acceptable Use for DHHS Information Systems Policy
  - DHHS Security Organization Policy
  - Security Training and Awareness Policy
  - Wireless Security Policy